Centre for Information Policy Leadership (CIPL)
and
Centro de Direito, Internet e Sociedade of Instituto Brasiliense de Direito Público (CEDIS-IDP)

Report of 2021 International Seminar:
International Dialogue on LGPD Implementation in the context of Global Data Protection

19, 20 and 21 May 2021

EFFECTIVE LGPD

Introduction

On 19, 20 and 21 May 2021, the Centre for Information Policy Leadership (CIPL) and the *Centro de Direito, Internet e Sociedade* of *Instituto Brasiliense de Direito Público* (CEDIS-IDP)[1] organized the International Seminar "International Dialogue on LGPD Implementation in the context of Global Data Protection." This was a **three-day event** consisting of four keynotes and three panels and followed by two invitation only roundtables under Chatham House Rule (hence not reported in this document).

The International Seminar gathered **37 panelists and moderators representing multiple stakeholder groups** to discuss the biggest data protection challenges around the globe including encouraging effective regulation, accountability and risk-based approach, enabling responsible international data flows, and other topics. The speakers represented global data protection authorities (DPAs), including the five Directors of the Brazilian DPA (ANPD), the US Federal Trade Commission (FTC), the Ireland Office of the Data Protection Commissioner (IDPC), the UK Information Commissioners' Office (ICO), the Singapore Personal Data Protection Commission (PDPC), the Japan Personal Information Protection Commission, the Belgian DPA, as well as policy-makers, privacy experts and leading multinational companies.

This Report details the key messages that were conveyed during the two open days of the International Seminar.

CIPL and CEDIS-IDP organized the International Seminar as part of our **Effective LGPD project**,[2] which was launched in July 2019 to explore topics related to the effective implementation and regulation under the new Brazilian data protection law (Lei Geral de Proteção de Dados-LGPD).

[1] CIPL is a global privacy and security think tank based in Washington, DC, Brussels and London. CIPL works with industry leaders, regulatory authorities and policy makers to develop global solutions and best practices for privacy and responsible use of data to enable the modern information age. Cedis/IDP is an institution focused on promoting research and debates on the implementation of new laws and regulations that impact the information society such as relating to privacy and data protection, competition and innovation, and internet governance. Cedis/IDP organizes events, workshops, research groups and partnerships with Brazilian and global organizations.

[2] CIPL-CEDIS Effective LGPD Project, available at https://www.informationpolicycentre.com/effective-lgpd.html.

Opening of Day One—Looking back six years and looking forward in data protection in Brazil and around the world

The world is currently experiencing the fourth industrial revolution, and the COVID-19 pandemic boosted this development and the data based innovations associated with it. **BOJANA BELLAMY**, President at CIPL, opened the International Seminar making remarks on this point. She outlined that the fourth industrial revolution is leading to the increase of international data flows and to the increase of new technologies such as Artificial Intelligence (AI) systems. As the ability to use AI depends on accessing data, processing it, and having large data sets for relevant purposes, this leads to tensions with data privacy rules that need to be properly understood and resolved. Coupled with this are a number of global developments, including (a) the EU GDPR, which has set a trend in data privacy regulation for many countries; (b) governments realizing the importance of data for economic and social purposes, (c) concerns about data transfers and data sovereignty; and (d) companies' boards increasingly taking responsibility for data uses.

LAURA SCHERTEL, Director at CEDIS-IDP, highlighted the latest data privacy developments in Brazil. She pointed out that the year 2020 was decisive in Brazil with the LGPD becoming applicable, the ANPD being established, and the Brazilian Supreme Court (STF) ruling that data protection is a fundamental right in Brazil. Laura flagged that stakeholders need to think about how to apply the LGPD to generate trust between companies, data subjects and the government in Brazil, as well as how the LGPD will be considered and applied in an international context. She mentioned that the partnership between CEDIS-IDP and CIPL is essential to help build an effective interpretation of LGPD.

Keynote 1—ANPD's regulatory agenda and priorities

WALDEMAR GONÇALVES ORTUNHO JR., President-Director at the ANPD, highlighted the importance of fostering a data protection dialogue in Brazil, in particular considering the recent creation of the ANPD and the challenges that the authority is currently facing. Despite the challenges of starting an authority and still having a staff of only 36 people, the ANPD has already undertaken relevant tasks such as publishing its Regulatory Strategy and Work Plan.[3] The ANPD created this strategy after analyzing similar work undertaken by other DPAs and understanding what is best practice from a regulatory perspective. Mr. Ortunho Jr. highlighted the importance of building a strong DPA in Brazil given the peculiarities of the country, and the need to have a flexible strategy and work plan that can be reviewed from time to time. He also called attention to the challenge of hiring qualified staff for the ANPD, and the opportunities that the ANPD is providing for their current staff to qualify through undertaking courses provided by third parties such as the European Commission.

Mr. Ortunho Jr. added that there is also the challenge of additional regulation, so they created a map of the topics and defined the Authority's priorities in order to form a solid regulatory agenda. This

[3] Available at https://www.in.gov.br/en/web/dou/-/portaria-n-1-de-8-de-marco-de-2021-307463618 and https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313.

does not mean that the ANPD will not also address other issues that are important or that might still appear on its agenda. One example is the issue of international data transfers. The development of the regulations will occur through public hearings and the submission of contributions from stakeholders. This methodology is being followed with respect to issues such as notification of security incidents, as well as developing specific approaches to compliance for small and medium-sized companies. Another ANPD action was regarding the privacy policy of WhatsApp, in which the ANPD, in collaboration with other bodies, had the opportunity to present a note on the update of the privacy policy. Finally, it was emphasized that the ANPD believes that the priority is to create a culture of data protection, raise awareness among the population, and highlight good practices for companies, all of which will be essential for applying the LGPD in a responsible and transparent way.

Keynote 2–Global and UK perspectives on data protection

According to **SIMON MCDOUGALL**, Executive Director, Technology Policy and Innovation and Deputy Commissioner at the UK Information Commissioner's Office (ICO), the COVID-19 pandemic has accelerated the urgency of existing data protection challenges and introduced new ones. We have seen a huge amount of innovation, for example, in the use of data to speed up vaccination programs and decrease virus transmission, as well as in the cases of vaccine passports and contact tracing applications. These contexts involved power imbalances with respect to access to and control over data, and more stakeholders have come to realize how much data permeates our lives.

Simon flagged that the broad scope of DPAs' work means that DPAs must be risk-based and prioritize their oversight and enforcement activities in order to effectively address increasing external demands and expectations. DPAs must also act based on solid principles, engage with multiple stakeholders, and be aware of the social and economic context purely beyond the legal context.

The ICO considers that although privacy is a fundamental right, it is not absolute and COVID has made this clear. Simon noted the impact of data processing on society and highlighted the need to maintain public trust in the data economy.

Finally, Simon acknowledged the need for the ICO to work with other regulators, legislators, and stakeholders in order to be effective. He flagged the creation of the Digital Regulation Cooperation Forum (DRCF) in the UK, which was created to enable cooperation between regulators in the areas of competition, communication, and data protection, and which resulted in the publication of a joint work plan.[4]

Panel 1—Regulation for results in data protection: cooperative engagement, effective oversight, smart enforcement

[4] Available at https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122.

Regulating for results involves making difficult, but essential, choices about strategies and priorities that are focused on the best outcomes for individuals, society and the economy. To operate effectively, DPAs need to prioritize and make strategic decisions, taking into account the data privacy areas that represent the highest risks to individuals. The goal of this panel was to discuss this ongoing journey and challenge for new DPAs (such as the ANPD) that are still grappling with setting up their operations, as well as for established DPAs.

ARTHUR SABBAT, Director at the ANPD, called attention to the first activity undertaken by the ANPD, which consisted on establishing its regulatory agenda. This agenda includes ten areas that were prioritized due to their potential impact on, and benefits to, society and individuals.

ANNA MORGAN, Deputy Commissioner of the Ireland Office at the Data Protection Commissioner, outlined that the Irish DPC is also setting priorities for its oversight and enforcement agenda. It is a challenge to manage and prioritize the authority's limited resources. She called attention to the difficulty of balancing the interests of various stakeholders and risks of data processing when dealing with society's demands for processing. Another significant problem is the large volume of complaints. Until May 2020, the Irish DPC analyzed all individual complaints it received and found that these complaints frequently related to labor or consumer areas instead of data protection or dealt with issues that did not have a significant, systemic or collective impact. A significant aspect of the DPC's work is to (a) help organizations understand their compliance obligations and to help them become compliant and accountable and (b) help empower individuals by educating them about their rights and entitlements. Finally, an important issue the DPC is grappling with is the practice of equating issuing large administrative fines with regulatory success and to measure success in terms of fines levied. "Hard enforcement" and sanctions are not the limit of what regulators can do; there are other tools and ways to achieve the desired outcomes of data protection, such as changing the underlying cultural approaches to data protection, which can be done by extensive engagement with regulated organizations. We need a balanced combination between the harder and softer approaches for achieving organizational accountability.

ZEE KIN YEONG, Assistant Chief Executive at the Singapore Personal Data Protection Commission, believes it is crucial to disseminate good practices in data protection and confirmed this has been a key activity for the Singapore PDPC. Enshrined in Singapore's data protection law is the PDPC's dual role of protecting personal data and enabling data use. He discussed knowledge sharing between the PDPC and the Singapore Institute of Directors, which is responsible for establishing corporate governance practices for companies in Singapore and which publishes a corporate governance handbook. The PDPC worked with the Institute of Directors to include data protection as one of the issues to which corporate boards need to pay attention. The PDPC also highlighted the good practices among companies that take part in certification schemes, given that companies have to be transparent towards the PDPC in order to obtain such certifications. Zee Kin Yeong noted that certifications are also a way of building companies' reputation in data privacy and create effective incentives for the adoption of good practices.

GUILHERME ROSCHKE, Counsel for International Consumer Protection at the Federal Trade Commission, said that two current data privacy issues are the discriminatory bias of algorithms in the face of flawed

tests and faulty inputs (e.g., the difficulty of facial recognition technology working efficiently with non-white individuals), and protecting youth data in the context of using technologies in education, which has significantly expanded during the COVID-19 pandemic. Mr. Roschke also talked about the importance of deterrence through enforcement in appropriate circumstances. Mr. Roschke highlighted the importance of encouraging transparency and accountability by organizations as key elements for addressing bad corporate behaviors but flagged that these should not create unreasonable burdens for individuals, such as overly lengthy privacy policies. He said that DPAs can use accountability as a tool to encourage companies to adopt good practices that will give them competitive and reputational advantages and help prevent enforcement actions. Finally, Mr. Roschke highlighted that in order to promote behavioral change, it is important to establish clear and transparent rules for companies (including about which practices are considered unfair), raise awareness of individuals of data protection issues and rights, and cooperate and share good practices with foreign counterpart authorities.

CHRIS HODGES, Head of the CMS Research Program on Civil Justice Systems at the University of Oxford, believes that there is a global trend for regulations to follow a risk-based approach and that this movement must be followed by actions focused on substantial behavioral change in the relationship between companies and individuals. That is because, as a rule, the motivation for change is linked to the behavior of individuals and not necessarily to the regulatory and punitive responses provided by law. Chris Hodges said that DPAs, therefore, have a role in communicating with key stakeholders, such as company Directors, to effectively influence behavior and encourage a risk- and outcome-based approach to resource allocation. Finally, he highlighted that codes of conduct should be encouraged as a way to promote a culture of data protection among companies.

EDUARDO BERTONI, representative and coordinator at the Regional Office of the Inter-American Institute of Human Rights for South America (IIDH) and former Director at the *Agência Argentina de Acesso à Informação Pública* (the Argentinian DPA), explained that one of the very first priorities of the Argentinian DPA was to make it as independent as possible. Until 2016, the DPA was linked to the Argentinian Ministry of Justice and Human Rights, and, therefore, its Directors could be dismissed at the discretion of the Minister of Justice. This called out the need for greater independence of the DPA, and the DPA started working to obtain such independence. Mr. Bertoni also believes that participation of the DPA in international fora strengthens its independence and benefits the DPA's activities relating to law enforcement. Mr. Bertoni highlighted that the LGPD should be implemented in a way that ensures greater autonomy for the ANPD.

Panel 2—The role of data privacy accountability: building risk-based data management programs and demonstrating compliance

Accountability is a key building block for effective privacy and data protection and is a key principle included in data protection laws around the world. It requires organizations to adopt and implement frameworks, systems, programs, practices, processes, policies and procedures, measures or tools (collectively, "mechanisms") to comply with legal requirements or other external standards, or to implement their own internal behavioral objectives, corporate ethics requirements, goals and public

promises. It also requires organizations to be able to demonstrate the effectiveness of such mechanisms internally (e.g., to the corporate board, CEO and other members of senior management) and externally (to DPAs, individuals, business partners, and increasingly, shareholders and investors). Organizations of all sizes, regions and industry sectors have been able to escalate and implement accountability in data privacy through data privacy management programs and expect DPAs to take such efforts into account during possible investigations and enforcement. The goal of this panel was to understand how companies are implementing accountability in data protection.

ROB SHERMAN, Vice President and Deputy Chief Privacy Officer at Facebook, stressed the necessity of thinking about international practices for accountability and oversight since many companies serve consumers worldwide and must adapt to the rules of many jurisdictions. Given the complexity of global privacy compliance, especially in light of legal and cultural differences, FB is using a regulatory implementation approach that divides the implementation of the laws into different subject matter areas, or thematic areas (e.g., consent and youth privacy), so that different groups are responsible for different issues. Mr. Sherman also stressed that it is crucial for organizational decision-making that DPAs are clear about their expectations with respect to specific compliance obligations, and that DPAs carry out external consultations. Finally, Mr. Sherman highlighted that investing in security and developing risk assessments play an essential role in accountability, as they help organizations to maintain consistency in their data processing activities and auditability over time.

CAROLINE LOUVEAUX, Chief Privacy Officer at Mastercard, affirmed that a data protection culture starts at the highest level of an organization. Mastercard has also implemented a series of measures of accountability, including data governance tools, compliance processes, a network of privacy officers, audits, as well as obtaining the Cross Border Privacy Rules Certification (CBPR). Ms. Louveaux believes that, for multinationals, it is more effective to have a single privacy program based on the highest privacy standards and adapt it to local jurisdictions, as opposed to having multiple, decentralized programs. She also flagged the importance of having a specific standalone policy about data breach management, to enable employees to have a clear understanding of the relevant processes and act quickly where needed. Finally, Ms. Louveaux highlighted the importance of training and awareness to create an accountability—and data protection culture within the organization.

RENATO MONTEIRO, Data Protection Counsel Lead for LATAM at Twitter, described a movement toward understanding privacy as a corporate objective. Consequently, privacy and information security have become part of the company's career advancement parameters and any interested employee can take a privacy certification. Another practice is to keep an open dialogue with regulators about the process of reviewing privacy practices; this occurred with the ICO, for example. Furthermore, Twitter indicates the legal basis for processing personal data and maintains the summaries of the legitimate interest assessment (LIA) publicly. The company retains the international privacy program at a global level, but increasingly regional approaches based on risks and benefits have been established.

ROBERTO BRUCE, Data Privacy Manager at Bradesco, said that accountability runs through the entire data protection regulation. In this sense, the LGPD encourages the adoption of good practices by processing agents. To understand and apply the principle of accountability, the company decided to work with the Brazilian Federation of Banks (FEBRABAN) to adopt the most recommended paths,

implement good practices, and produce informative videos and courses. Furthermore, the board appointed a data protection officer (DPO) and indicated the name and contact of the DPO on the bank's website in addition to creating means for data subjects to exercise their rights.

MARLON DOMINGUES, Data Protection Officer at Erasmus University Rotterdam, noted that for companies to implement accountability, it is necessary to establish leadership to conduct the compliance program and develop privacy policies and other updated and specific standards. This must be ensured within a specific and comprehensive framework that underlies the privacy compliance program, such the CIPL Accountability Framework. Using such a formal framework will provide the necessary structure necessary for an organization in the education sector (or otherwise), to ensure compliance at three levels: within the organization, in international collaborations, and the higher education sector. He also noted that the Dutch DPA has adopted the CIPL Accountability Framework for its upcoming report with snapshots of the privacy governance in the different sectors in the Netherlands.

TAMI DOKKEN, Chief Data Privacy Officer at the World Bank, said that although the World Bank is an international organization, which is exempt from following any country-specific regulations such as the GDPR or the LGPD, the institution realizes the risks of ignoring issues regarding the use of personal data, specifically in research conducted by the bank. These risks include legal, business and reputational risks. The bank voluntarily created its first personal data privacy policy in 2018 and it went into effect in February 2021. Specifically on accountability, the Bank's privacy policy requires accountability both internally and externally, and the data privacy governance is used with the standard three lines of defense model in which all staff is responsible for integrating data privacy into their daily work. Moreover, the bank has conducted a risk assessment of every business unit region and practice group to identify the organization's activities that involve personal data.

MARCOS OTTONI, Legal Coordinator at CNSaúde, highlights that the health sector is called upon to adapt its internal policies, implement privacy guidelines, and use personal data to fight the pandemic rationally. Therefore, the organization noted the possibility of providing good practices at the individual level and in associations. Considering this, CNSaúde launched the Code of Good Practices for Private Providers in Health.[5] The establishment of this privacy policy between the organizations that compose CNSaúde serves both to protect the data subjects, guarantees commercial symmetries, and avoids competitive distortions. The code of good practices is not a static text that does not observe concrete and new issues. Thus, it is essential to act alongside public authorities so that the problems are debated in a reasoned manner.

Opening Day Two

GIOVANNA CARLONI, Global Privacy Policy Manager at CIPL and **LAURA SCHERTEL**, Director at CEDIS-IDP, highlighted the link between the discussions of the first and second days of the international seminar,

[5] Available at http://cnsaude.org.br/baixe-aqui-o-codigo-de-boas-praticas-protecao-de-dados-para-prestadores-privados-de-saude/.

since accountability and effective regulation are essential to enable trusted international data flows and for the good management and prevention of data breaches.

Keynote 3—Data Protection Officers and the rise of the data privacy profession around the globe

The first speaker was **TREVOR HUGHES,** CEO and President at the International Association of Privacy Professionals (IAPP), the world's largest community of data protection professionals. Mr. Hughes talked about the fact that the professionalization of those involved in data processing is central to effective data protection, and that the GDPR has emphasized this need. In Brazil, for example, it is estimated that 50,000 professionals will be needed in the area of data protection. In this context, a well-trained professional is essential, adding great value to data protection and the digital economy. Thus, he explained that the main function of the IAPP is precisely to create mechanisms, such as training and the increase of higher education courses in this field, in order to train DPOs and other professionals that work with personal data.

Keynote 4—Creating a pro-growth and trusted data regime under the UK's National Data Strategy

JAMES SNOOK, Director of Data Policy at the UK's Department for Digital, Culture, Media and Sport (DCMS), focuses mainly on the development of data protection regulations is his role at DCMS. In the presentation, he dealt mainly with the UK's National Data Strategy, published in 2020. The importance of the document was justified on three grounds: (i) the economic value of data in modern times; (ii) the value of such assets to public institutions to improve their efficiency; and (iii) the risks arising from data processing to individual rights.

Thus, the main objective of the Strategy consists in minimizing the risks and maximizing the opportunities arising from new technologies and data processing. To this end, he separated the National Strategy into five missions:

(i) to ensure an environment where the economic value of data can be thoroughly exploited;
(ii) create a pro-growth environment that considers the limitations of each organization to define its data protection obligations;
(iii) maximize public efficiency in the performance of their services through data processing;
(iv) establish a strong risk management framework, in light of our increasing dependence on technology and data processing; and
(v) create a strong legal and regulatory framework for establishing a secure environment for international data transfer, placing the UK as an international leader for the development of this pillar.

Panel 3—Enabling international data transfers across regions

International data transfers enable digital development and innovation and are key to enabling developing countries such as Brazil to effectively participate in the global digital economy. They are also key to combating global crisis situations such as the COVID-19 pandemic. Countries and regions are adopting mechanisms to facilitate the cross-border flow of personal data, including mutual adequacy recognition, bilateral agreements, certification schemes, contractual clauses and others. Increasingly, local decisions on data protection have a broader and sometimes even global impact on data flows, such as the decision by the Court of Justice of the European Union in the *Schrems II* case, adding complexity to the issue of data flows and requiring countries to observe and analyze the impact of data privacy developments that happen beyond their physical borders.

MIRIAM WIMMER, Director at the ANPD, explained that data protection is an incipient subject in Brazil, which makes the discussions move at a slower pace. Even so, she said that the ANPD is setting priorities for the development of the subject in Brazil; among them, the cross-border flow of data, which has regulatory space planned for the first half of 2022, according to the regulatory agenda published by the Authority. In this context, Ms. Wimmer closed her presentation stating that the initial scope will be a regulation focused on the practice of data transfer in the daily life of companies, the most straightforward and urgent issue.

YUJI ASAI, Commissioner, Personal Information Protection Commission of Japan, discussed the mutual recognition between Japan and the European Union for the free flow of data, stating that this is achieved through trust, which is built on similar data protection structures, regardless of cultural differences between countries or regions. Lastly, he explained the existence of certificates that allow the free flow of data, which attests to the trust between countries, and which may serve Brazil in the future.

JOE JONES, Head of Data Adequacy at the UK DCMS, discussed the need for a culture of data protection, which varies from country to country depending on their background. In this regard, he pointed out that to establish mutual adequacy for the free flow of data, there is no need for correspondence in the regulations themselves, but there is a need for identity in the data protection framework and in the general principles that guide it. In addition, he stressed that the adequacy process must take place with a sense of mutuality and a cooperative spirit, not with one country or region providing rules that the other must accept. The agreement with Japan is an example in this sense, as it was conducted with much dialog.

KATE CHARLET, Director for Data Governance at Google, talked about the importance of global computing. According to her, the interconnected network around the globe helps in information security, assisting, for example, in mapping the flow of data in a system. This shows that global free flow of data does not necessarily constitute a threat to data protection but improves data protection. Furthermore, Ms. Charlet highlighted the importance of the free flow of data for society, going from the advantages that all companies find when there are no barriers to this flow to the benefits that this brings to consumers. She noted the importance of cross-border certification mechanisms, such as the APEC Cross-Border Privacy Rules (CBPR), as a way to create global interoperability between legal systems while maintaining a high level of protection.

JACOBO ESQUENAZI, Global Privacy Strategist at HP, Inc., talked about certificates of trust issued by some countries for companies. Mr. Esquenazi affirmed that this is an excellent instrument for compliance with the strictest data protection and transfer standards, since, for global compliance, the company will have to use a code of conduct that is adapted for or usable in all of the regions where it operates. He noted the relevance of the APEC CBPR in that connection but said that it is important that such an interoperability code of conduct or certification must be global to truly meet the needs of businesses. He advised Brazil to approve or recognize the certificates that already exist, such as the CBPR, and welcomed their possible globalization.

MARCEL LEONARDI, Partner at Leonardi Advogados, discussed the issues arising from the absence of mechanisms for international data transfers in the Brazilian regulatory context, in view of the incessant need for companies to carry out cross-border data processing operations. Between following the European legislation for data transfer and other possibilities, Mr. Leonardi pointed out that the best alternative is for companies to establish an intense debate with the ANPD so that it might provide guidelines for cross-border data transfers while there are no solid regulations or other instruments on the subject.

Panel 4—Reporting and managing data breaches and notifications: a challenge for both organizations and DPAs

Identifying and managing data breaches is a challenging task both for organizations and DPAs. As the world has gone digital with the COVID-19 pandemic, cyber threats and attacks have increased, leading to an increase in data breach management and notification. While organizations work to implement enhanced technical and organizational measures to prevent and contain breaches, they are also required to notify such breaches to DPAs and individuals across multiple jurisdictions. DPAs in various regions have seen an increase in their workload due to data breach notifications. They need to spend resources in analyzing such notifications, providing guidance to organizations so that they have clarity concerning the notification criteria, and possibly investigating and taking enforcement measures against the more severe cases.

JOACIL BASÍLIO RAEL, Director at ANPD, emphasized the seriousness that data breaches can have, especially when they involve sensitive data, generating irreversible individual and collective damage. He stated that, with this context in mind, the ANPD adopted as a priority the regulation of data breaches and its notification, and that, in 2021, a Call for Proposals was launched by the Authority in order to provide guidance to civil society, which will lead to complementary normatives.

DAVID STEVENS, Chairman at the Belgian Data Protection Authority, stated that, based on Belgium's experience after the GDPR came into force, it is common for data breach notifications to increase once the data protection regulation is in place. In this regard, he pointed out the importance of certain measures, such as (i) having good organizational standards, for instance through the implementation of software that separate and organize incoming notifications, (ii) being able to select and give more attention to what is important and has learning potential, and (iii) communicating to society about data breaches with caution, providing only the right information about the case, without a lot of fuss.

BRIDGET TREACY, Partner at Hunton Andrews Kurth, pointed out that data breaches are part of the daily routine of companies; they are not going to disappear, the companies must learn how to deal with them. To do so, she highlighted that, first of all, companies must learn to identify the incident, which is often an overwhelming task; next, she emphasized the importance of internal reporting mechanisms, i.e., encourage the use of reports within the company itself to communicate what happened; finally, she highlighted the difficulty and the short period of time to notify those affected by the data breach, considering the complexity of many cases. On this last point, she emphasized the importance of the Authorities understanding that the first communication about the data breach will be shallower, while the company deals with better understanding of what occurred.

FLAVIA MITRI, LATAM Legal Director Privacy & Cybersecurity at Uber, talked about the company's experience and the many difficulties the company has faced in connection with reporting data breaches. She affirmed that, over time, it has built a solid and prepared team to deal with breaches, and the teams work all over the world, complying with the specific rules of the site where the problem was detected. Another point of emphasis concerns the difference in communication about data breaches to the data subjects and to the authorities. For the latter, Ms. Mitri noted that the communication is technical and only occurs when it is legally necessary; as for the data subjects, she stated that the company values a more humanized and careful communication, which occurs regardless of legal requirements.

MARIE OLSON, Deputy Chief Privacy Officer at Boeing, discussed the importance of adopting an action plan even before a data breach occurs, so that the company will have the whole structure ready to execute each of the necessary steps to address the problem. For example, one group will be trying to correct the incident, while another will be investigating the causes, and another will be informing the relevant people or DPAs. She also highlighted details that are important to avoid data breaches, such as encrypting laptop disks, and even giving employees tips on how not to have their machines stolen, such as not leaving them in the front seat of the car or not taking them on trips where they are not needed.

NICOLAS ANDRADE, Head of Government Relations for Latin America at Zoom, talked about the need to invest in a strong privacy team that develops its work in an integrated way with the rest of the company, an approach adopted by Zoom, especially because of the great increase in demand during the pandemic. Moreover, the executive highlighted other important features, such as increasing the time for reporting data breaches to the data subjects and simplifying the breach notification forms, removing, for example, the need for the CPF/CNPJ of the data controller, since there are companies that are not physically located in Brazil.

CRISTINE HOEPERS, General Manager at CERT.br/NIC.br, highlighted the importance of data breach management and its intersection with information security. Cristine believes that it is extremely important to know what to do before and after data breaches occur, and flagged the relevant role of a data breach management group and of the DPO, whose expertise should go beyond data protection and cover technical skills that are useful for the prevention and control of data breaches.